FORRESTER®

Mind The Gaps

Proactive Investments In Security Operations Improve Breach Readiness And Response Capabilities

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY ARCTIC WOLF | JANUARY 2023

Overview
Situation
Challenge
Opportunity
Conclusion

Improving Cybersecurity Capabilities Requires Proactive And Strategic Approaches

Cybersecurity incidents can cause catastrophic damage to organizations from distracting organizational efforts away from business priorities to depleting resources. This requires tech executives to rethink and re-evaluate their approach to cybersecurity.[1] As cybersecurity leaders grapple with this reality, they find a lack of satisfaction with their organizations' current cybersecurity capabilities.

To mitigate the impact of cybersecurity incidents on organizations, staffing shortages, technical issues, and budget challenges must be addressed. This includes creating a renewed proactive approach to cybersecurity strategies and the development of partnerships to fill organizational gaps.

Key Findings

Security leaders are looking for more. While security leaders increased investments in cybersecurity, most are not satisfied with their current security capabilities.

Threat detection and response is a top gap. Staffing, technical skills, and budget challenges are the biggest obstacles for improving security, leaving organizations unprepared for threat detection and response.

Proactiveness and partners enable success. Proactive security practices are expected to enable better threat detection and improve mitigation and response time with security partners filling staffing and knowledge gaps.

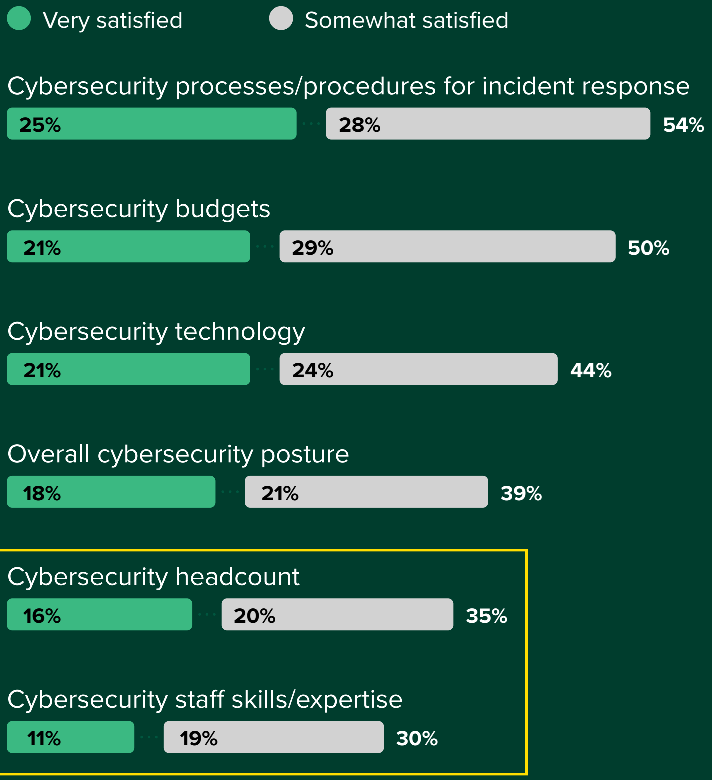
Overview
Situation
Challenge
Opportunity
Conclusion

Satisfaction With Current Security Capabilities Is Lacking

Cybersecurity leaders are striving to improve their breach readiness and responsiveness. But current cybersecurity capabilities fail to impress. Just above half of surveyed respondents are “Somewhat satisfied” or “Very satisfied” with cybersecurity processes and procedures, as well as budgets. Achieving the necessary headcount and right staff skills/expertise is where respondents were least satisfied with current capabilities.

With small teams of full-time employees, which are predominantly dedicated to SecOps (35% on average) and application security (42% on average), a majority (81%) do not have 24/7 security coverage. With that, 33% report they are actively working to achieve full 24/7 coverage.

“How satisfied are you with your company’s current cybersecurity capabilities?”



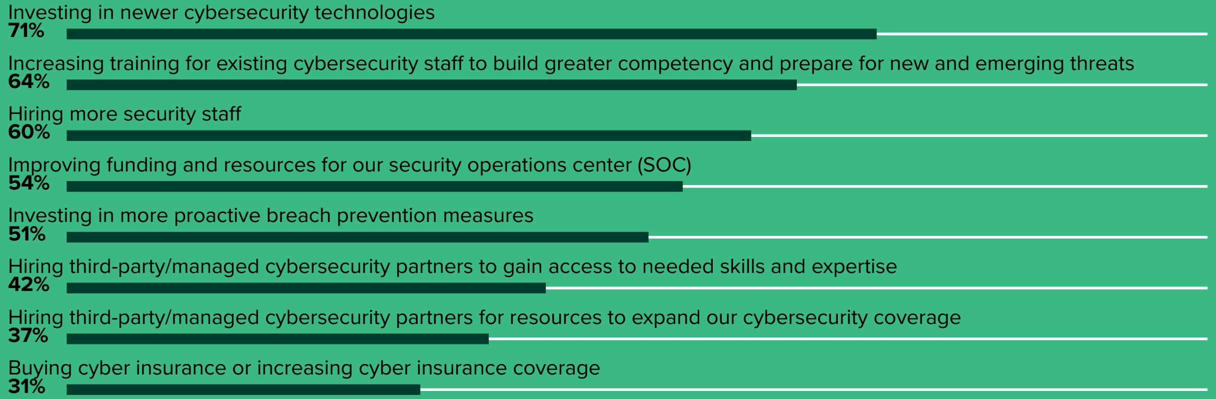
Base: 209 North American cybersecurity decision-makers
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Arctic Wolf, October 2022

After The Breach Comes The Investment

Sixty-four percent of surveyed cybersecurity decision-makers report their organizations experienced a breach in the past year. In order to counteract the rise in breaches, organizations are making investments to better defend against cyberthreats and mitigate the impacts of a breach, including enhanced cybersecurity technologies, increasing staff skills through training, hiring more staff, and improving funding and resources for the SOC.

When focusing on the most proactive approach to investments — those which are part of an overall strategy to improve breach readiness — cybersecurity leaders are most focused on hiring more security staff (47%), hiring the right partners to access needed skills and expertise (43%), and increasing training of existing staff for greater competency (41%).

“What cybersecurity investments has your organization made in the past year or is making now to defend against cyberattacks and/or mitigate the impacts of a breach?”



Base: 209 North American cybersecurity decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Arctic Wolf, October 2022

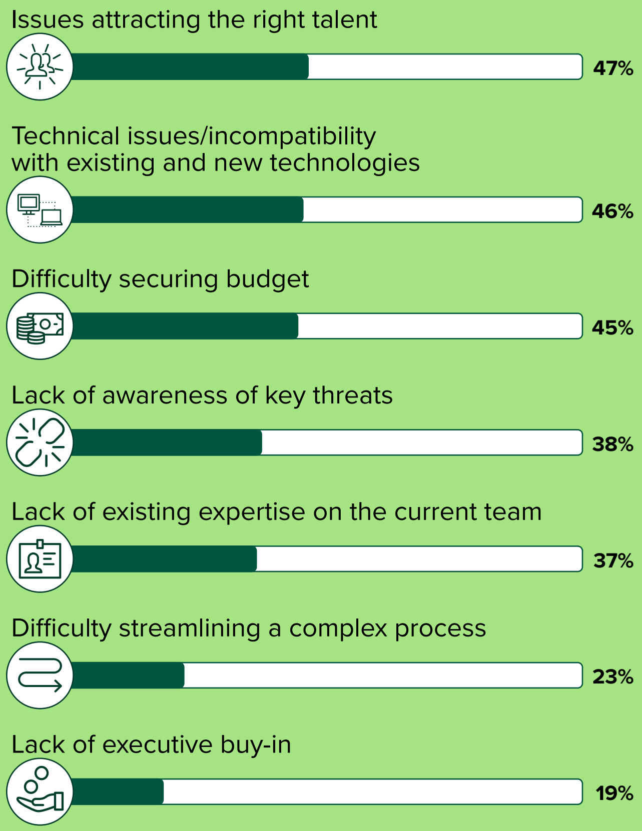
Overview
Situation
Challenge
Opportunity
Conclusion

Challenges With Staffing, Technology, And Budget Hamper Threat Detection And Response

While security improvements are typical year after year, cybersecurity leaders continue to feel unprepared. The top concerns reported are a lack of preparedness surrounding threat detection and threat response, followed by incident/breach recovery. The top impediments to improving organizations cybersecurity capabilities? Staffing, tech incompatibility issues, and budget challenges.

When setting cybersecurity budgets, minimum levels of requirements from cyber insurance providers and technology needs are the most common considerations that cybersecurity leaders need to account for.

"What is inhibiting your organization from improving its cybersecurity capabilities?"



Base: 209 North American cybersecurity decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Arctic Wolf, October 2022

Overview
Situation
Challenge
Opportunity
Conclusion

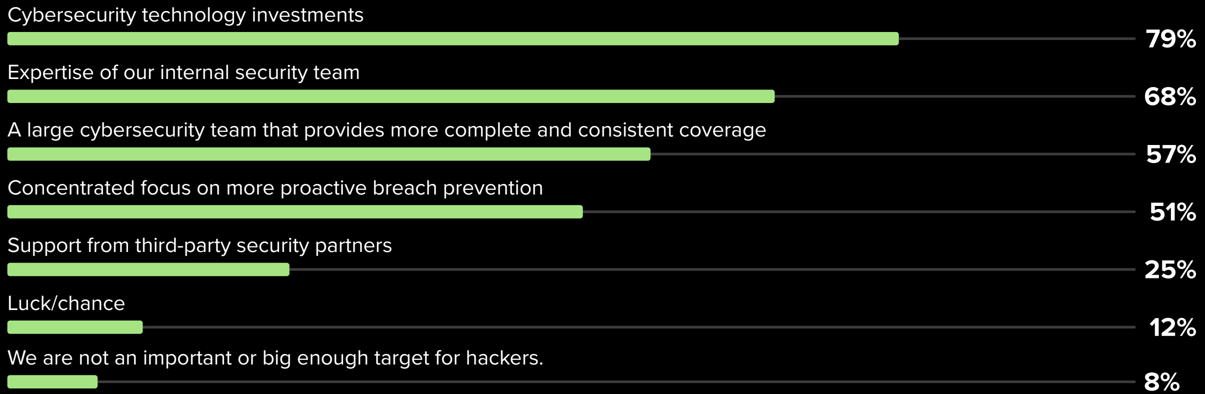
Readiness And Response Requires The Right Mix

Organizations that have not experienced a recent breach attribute their success to technology investments (79%) and their security teams' expertise and size (68%).

Successful readiness and response to a cybersecurity breach requires a mix of the right people, processes, and technology initiatives. To improve their readiness and response to a cybersecurity breach, organizations are planning proactive prevention through staff training, implementing a more proactive security strategy, upgrading cybersecurity technology, and hiring additional cybersecurity staff.

Organizations that have not experienced a recent breach attribute their success to technology investments and their security teams' expertise and size.

(Showing "Top 3 ranked" responses)



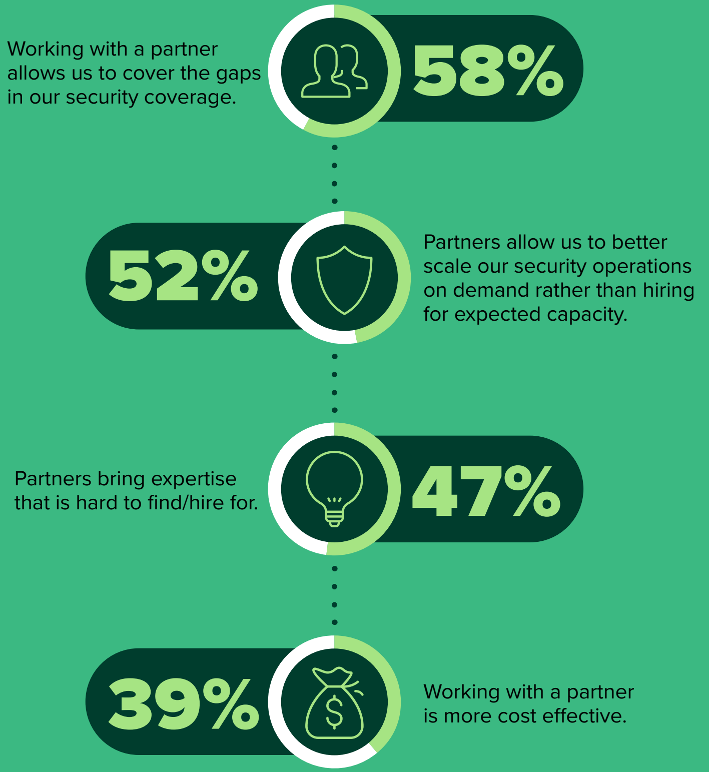
Base: 75 North American cybersecurity decision-makers who work at organizations who have not experienced a cybersecurity breach within the past year
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Arctic Wolf, October 2022

Overview
Situation
Challenge
Opportunity
Conclusion

Partnership With External Security Partners Fills Existing Security Coverage Gaps

Sixty-five percent of surveyed leaders report their companies are working with external security partners to fill skills and staffing gaps. The primary reasons for using third-party partners, such as managed security services and managed detection and response (MDR) providers, versus internal resources? Addressing gaps in security coverage, better scaling of security operations on demand, access to needed expertise, and cost effectiveness.

Using Partners Covers Security Gaps And Gives Access To Hard-To-Find Skill Sets



Working with a partner allows us to cover the gaps in our security coverage. 58%

52% Partners allow us to better scale our security operations on demand rather than hiring for expected capacity.

Partners bring expertise that is hard to find/hire for. 47%

39% Working with a partner is more cost effective.

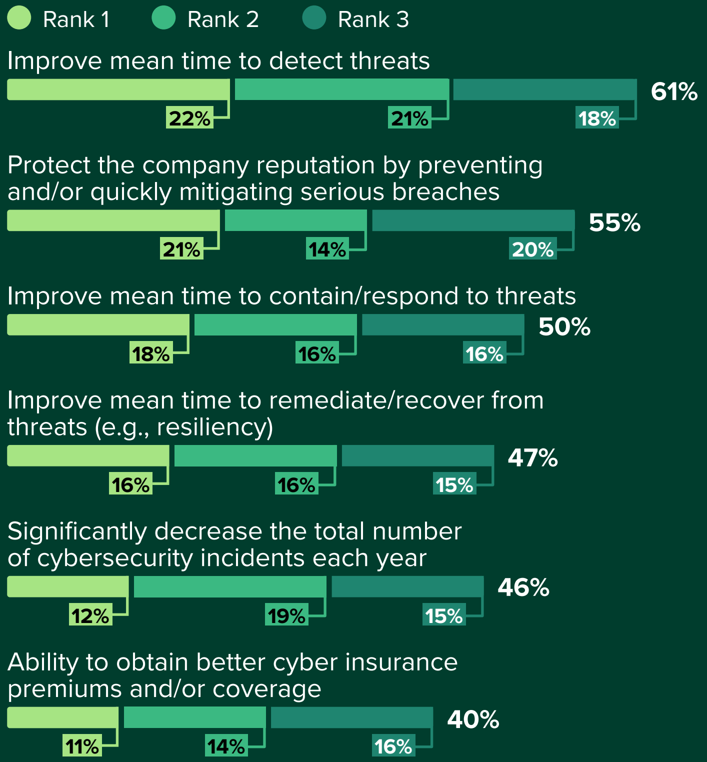
Base: 135 North American cybersecurity decision-makers whose companies use third-party partners to support cybersecurity operations
Source: A commissioned study conducted by Forrester Consulting on behalf of Arctic Wolf, October 2022

Overview
Situation
Challenge
Opportunity
Conclusion

Increased Proactivity Improves Threat Detection And Mitigation

As companies continue to implement more proactive cybersecurity breach mitigation and prevention capabilities, organizations are eager to experience the benefits, namely speedier thread detection, containment, and remediation, as well as protection of the company reputation.

"Which of the following outcomes are most important to you as your company implements more proactive cybersecurity breach mitigation and prevention capabilities?"



Base: 209 North American cybersecurity decision-makers
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Arctic Wolf, October 2022

Conclusion

As cybersecurity leaders work to improve their organizations' breach readiness and responsiveness, they must make the right investments and strategy decisions to overcome security challenges and recenter focus on organizational priorities (vs. cybersecurity priorities).

While organizations have been investing in security practices each year, most cybersecurity leaders are not satisfied with their organizations' current cybersecurity capabilities.

Threat detection and response challenges are top of mind, leaving organizations feeling unprepared. These are impeded by staffing gaps, technical issues, and budget challenges.

Opportunities to mitigate risks related to insufficient threat detection and response include implementing proactive security practices and strategy, along with the right security partners to address staff and knowledge gaps.

Project Director:

Chris Taylor,
Principal Market Impact Consultant

Contributing Research:

Forrester's Security and Risk research group

Methodology

This Opportunity Snapshot was commissioned by Arctic Wolf. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 209 North American cybersecurity decision-makers. The custom survey began and was completed in October 2022.

ENDNOTES

[1] Source: “The State Of Privacy And Cybersecurity, 2022,” Forrester Research, Inc, September 8, 2022.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester’s seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Demographics

COUNTRY	
United States	**60%**
Canada	**40%**

CURRENT POSITION	
Chief information officer	**12%**
Chief information security officer	**12%**
Chief security officer	**13%**
Business information security officer	**8%**
Chief technology officer	**18%**
VP in IT or cybersecurity	**19%**
Director in IT or cybersecurity	**19%**

COMPANY SIZE	
1,000 to 4,999 employees	**23%**
5,000 to 9,999 employees	**27%**
10,000 to 19,999 employees	**32%**
20,000 or more employees	**19%**

TOP 5 INDUSTRIES	
Retail	**10%**
Transportation and logistics	**9%**
Telecommunications services	**8%**
Travel and hospitality	**8%**
Healthcare	**7%**

Note: Percentages may not total 100 because of rounding.

FORRESTER®